JOURNAL OF ALGEBRA 32, 554–560 (1974)

A Unitary Version of the Brauer–Cartan–Hua Theorem

I. N. HERSTEIN*

University of Chicago, Chicago, Illinois 60637

Received November 8, 1973

A well-known result, often called the Brauer–Cartan–Hua Theorem, states that if a subdivision ring A of a division ring D is invariant with respect to all the inner automorphisms of D, in the sense that $xAx^{-1} \subset A$ for all $x \neq 0$ in D, then either $A = D$ or $A \subset Z$, the center of D (see, for instance, [1]). This result has been generalized in a variety of directions. In this paper we give an extension of the Brauer–Cartan–Hua Theorem in a somewhat different direction, that of division rings endowed with an involution. The result arose in a context quite different from that of division rings, coming out of a study we were making of certain rings of operators on a Hilbert space. In that setting the analogous question remains open.

Let D be a division ring and let Z be its center. Suppose that D has an involution *, that is, a mapping *: $D \to D$ which satisfies the usual properties: $a^{**} = a$, $(a + b)^* = a^* + b^*$, and $(ab)^* = b^*a^*$, for all $a, b \in D$. An element $a \in D$ is called *symmetric* if $a^* = a$; we shall denote the set of symmetric elements of D as S. An element $a \in D$ is called *skew* if $a^* = -a$; we shall denote the set of skew elements of D as K. Finally, an element $a \in D$ is called *unitary* if $aa^* = 1$.

If the characteristic of D is not 2, then we have the Cayley parametrization for the unitaries of D. Namely, if u is unitary then $u = (1 - k)(1 + k)^{-1}$ for some $k \in K$; moreover, every $(1 - k)(1 + k)^{-1}$, with $k \in K$, is unitary. Thus, in this case, we have a rather large supply of unitaries. In characteristic 2 the story is quite different. P. M. Cohn has given an example, in that case, where 1 is the only unitary element of D.

In what follows, we shall be concerned with a division ring D with involution *of characteristic different from* 2. The question we propose to study is the following: Suppose that A is a subdivision ring of D such that $uAu^{-1} \subset A$ for all unitaries $u \in D$; does it then follow that $A = D$ or $A \subset Z$? As we shall soon see, the answer in general is yes.

Before we attempt to prove, or even to state, the exact theorem, let us

* The research in this paper was supported by an NSF grant GP-2969 at the University of Chicago.

look at two special cases. If D is 4-dimensional over Z, then we can introduce an involution on D such that the skew elements form a 1-dimensional space over Z. In this situation we can produce a commutative subfield of D, which is not in Z, which is invariant with respect to the unitaries of D. If D is 16-dimensional over its center, as we shall see in the proof, we cannot find a noncentral commutative subdivision ring which is invariant with respect to the unitaries of D. However, we can construct a proper, noncommutative subdivision ring which is invariant with respect to the unitaries of D. To see this, pick A and B which are 4-dimensional division algebras over a field F, such that $A \otimes_F B$ is again a division algebra (this can be done for appropriate F). Using the usual involutions on A and B—that in which all the symmetrics are central—then it can be verified that $A \otimes 1$ is invariant with respect to all the unitaries of $A \otimes_F B$.

In what follows A will be a subdivision ring of D such that $uAu^{-1} \subset A$ for all unitary elements u in D.

We begin with the following:

LEMMA 1. *If $a \in A$ and $k \in K$ then $(1 - k)^{-1}(ka - ak)(1 + k)^{-1} \in A$.*

Proof. Let $u = (1 + k)(1 - k)^{-1}$; then u is unitary. We can write u as $u = 1 + 2k(1 - k)^{-1}$; thus $u^{-1} = u^* = 1 - 2k(1 + k)^{-1}$. If $a \in A$, then from $uau^{-1} \in A$ we obtain $(1 + 2k(1 - k)^{-1})\, a(1 - 2k(1 + k)^{-1}) \in A$. Expanding this and simplifying yields that $(1 - k)^{-1}(ka - ak)(1 + k)^{-1} \in A$, the desired result.

Clearly the lemma does not depend on the fact that D is a division ring. It holds for any ring provided $1 - k$, $1 + k$ are invertible and if $2x \in A$ then $x \in A$.

We go on to the following:

LEMMA 2. *If $a \in A$, $k \in K$ and $ak - ka \neq 0$, then, if $b = (ak - ka)^{-1}$:*

(1) *$kb - bk \in A$ and*

(2) *$b - kbk \in A$.*

Proof. By Lemma 1, $(1 - k)^{-1}(ka - ak)(1 + k)^{-1} \in A$, hence, since $ka - ak \neq 0$, $((1 - k)^{-1}(ka - ak)(1 + k)^{-1})^{-1} \in A$. This yields $(1 + k)\, b(1 - k) \in A$, that is, $b - kbk + kb - bk \in A$. But $-k$ is also skew; using it instead of k, b becomes $-b$ and the result above yields $b - kbk - (kb - bk) \in A$. Combining these two results gives $2(kb - bk) \in A$ and $2(b - kbk) \in A$. Since the characteristic is not 2 and A is a subdivision ring, we end up with $kb - bk \in A$ and $b - kbk \in A$, as required.

At this point, we can easily derive the final theorem we want, if the characteristic of D is also not 3. For replacing k by $2k$ in $b - kbk \in A$,

b becomes $\frac{1}{2}b$, hence $\frac{1}{2}b - (2k)(\frac{1}{2}b)(2k) \in A$, that is, $b - 4kbk \in A$. Thus $4(b - kbk) - (b - 4kbk) = 3b \in A$, whence $b \in A$. Hence $b^{-1} = ak - ka \in A$, if $ak - ka \neq 0$. On the other hand, if $ak - ka = 0$ it certainly is in A. Thus $[A, K] \subset A$. By [2] we would have that $A \subset Z$ or $A = D$ provided the proper conditions on $\dim_Z D$ are imposed.

However, until the final moments of the proof, the characteristic does not make its presence felt, and there is little gain in assuming that the characteristic is 3. So we continue with no qualification on the characteristic of D, other than char $D \neq 2$.

The involution $*$ is called of the *second kind* if $\lambda^* = -\lambda \neq 0$ for some $\lambda \in Z$.

LEMMA 3. *If $*$ is of the second kind then $[A, K] \subset A$.*

Proof. If $[A, K] = 0$ then $[A, K]$ is certainly in A. Suppose that $ak - ka \neq 0$ for some $a \in A$, $k \in K$. If $b = (ak - ka)^{-1}$ then, by Lemma 2, $b - kbk \in A$. If $\lambda^* = -\lambda \neq 0$ is in Z, then $k + \lambda$ is skew and with a gives rise to the same b; hence $b - (k + \lambda)\, b(k + \lambda) \in A$. Similarly,

$$b - (k - \lambda)\, b(k - \lambda) \in A.$$

Playing these off against each other we get $\lambda^2 b \in A$, thus $(\lambda^2 b)^{-1} = \lambda^{-2}(ak - ka) \in A$. Since $\lambda^{-2}K = K$, we get from this that $[A, K] \subset A$.

LEMMA 4. *If A consists only of symmetric elements, and if $\dim_Z D > 4$, then $A \subset Z$.*

Proof. Since A consists only of symmetric elements, it must be commutative. If $A \not\subset Z$, then since $\dim_Z D > 4$, there is an $a \in A$, $k \in K$ such that $ak - ka \neq 0$. If $b = (ak - ka)^{-1}$ then, by Lemma 2,

(1) $kb - bk \in A$ and $b - kbk \in A$.

Since $a^* = a$, $k_1 = aka \in K$ and $k_1 a \neq ak_1$. Moreover, $c = (k_1 a - ak_1)^{-1} = -a^{-1}ba^{-1}$. By Lemma 2, $k_1 c - ck_1 \in A$, that is

(2) $akba^{-1} - a^{-1}bka \in A$.

But, from (1), $akba^{-1} - abka^{-1} \in A$; together with (2) this gives

$$abka^{-1} - a^{-1}bka \in A,$$

hence

(3) $bka^2 - a^2bk \in A$.

Since $a + 1 \in A$ and gives rise to the same b, substituting $a + 1$ for a in (3) and subtracting (3) gives us

(4) $bka - abk \in A$.

Now, $abk - kab = (ak - ka)b + (ab - ba)k = 1 + (ab - ba)k$; the net result of this is

(5) $(ab - ba)k \in A$.

Since $kb - bk \in A$, it must commute with a. Because $(ak - ka)b = 1$, we get from this that $(ab - ba)k = k(ab - ba)$. Also, since $b - kbk \in A$, it commutes with a. Working this out, using that $(ab - ba)k = k(ab - ba)$, we get $ab - ba - 2k - (ab - ba)k^2 = 0$, hence

(6) $ab - ba = 2k(1 - k^2)^{-1}$.

From (5) we then get that $2k^2(1 - k^2)^{-1} \in A$, hence $k^2(1 - k^2)^{-1} \in A$. But then $(1 + k^2(1 - k^2)^{-1})^{-1} = 1 - k^2 \in A$, whence $k^2 \in A$, and so $k^2a = ak^2$. Thus, if $ka \neq ak$ then $k^2a = ak^2$. In short, $k^2a = ak^2$ for all $a \in A$, $k \in K$. But, by Theorem 2.3 of [3], the additive group generated by all k^2 is S, hence A centralizes S, if $\dim_Z D > 4$. But, since $\dim_Z D > 4$, S generates D by Theorem 1.6 of [3]. Thus we get $A \subset Z$.

We are now able to prove the unitary version of the Brauer–Cartan–Hua Theorem.

THEOREM. *Let D be a division ring with involution $*$, of characteristic not 2. Let A be a subdivision ring of D such that $uAu^{-1} \subset A$ for every unitary element $u \in D$. Then*

1. *If A is commutative and $\dim_Z D > 4$, $A \subset Z$ the center of D.*
2. *If A is noncommutative and $\dim_Z D > 16$, $A = D$.*

Proof. We first prove the theorem for subdivision rings A such that $A^* = A$, (i.e., $a^* \in A$ for all $a \in A$). From this we shall pass to the general case.

Suppose, then, that $A^* = A$ and $uAu^{-1} \subset A$ for every unitary $u \in D$. If every element in A is symmetric, by Lemma 4 we have that $A \subset Z$. Thus we may suppose that A has nonzero skew elements. Hence, if $A^- = A \cap K$, then $A^- \neq 0$.

If $A^- \subset Z$ then we claim that $A \subset Z$. For let $\lambda \neq 0$ be in A^-; if $s^* = s$ is in A, $(\lambda s)^* = -\lambda s$, so $\lambda s \in A^- \subset Z$. Thus we get $s \in Z$. Hence $A \cap K \subset Z$ and $A \cap S \subset Z$. But, since $A^* = A$, $A = (A \cap K) + (A \cap S) \subset Z$.

Therefore we may suppose that $A^- \not\subset Z$. Since $\dim_Z D > 4$, by Theorem 2.13 of [3], K generates D. Thus, since $A^- \not\subset Z$, there is an $a \in A^-$, $k \in K$ such that $ak - ka \neq 0$. Let $b = (ak - ka)^{-1}$. By Lemma 2, $b - kbk \subset A$.

Now $k \pm a$ are both in K, and these commute with a to give the same b above. Therefore $b - (k + a)\, b(k + a) \in A$ and $b - (k - a)\, b(k - a) \in A$. These combine to give $2aba \in A$, hence $aba \in A$. But then $b \in A$ since A is

a subdivision ring; in consequence, $b^{-1} = ak - ka \in A$. Thus $a \in A^-$, $k \in K$ implies that $ak - ka \in A$. Since $ak - ka \in K$, we have $ak - ka \in A^-$. In other words, $[A^-, K] \subset A^-$, and A^- is a Lie ideal of K.

If A is not commutative, and $\dim_Z D > 16$, then by Theorem 2.12 of [3], A^-, as a Lie ideal of K, must satisfy $A^- \subset Z$ or $A^- \supset [K, K]$. We already saw that $A^- \subset Z$ forces A to be commutative. Hence $A^- \supset [K, K]$. But, by Theorem 2.13 of [3], $[K, K]$ generates D, and since $[K, K] \subset A^- \subset A$, we get $A = D$.

Suppose then that A is commutative and $\dim_Z D > 4$. Since A^- is a Lie ideal of K, by Theorem 2.9 of [3], since A^- is commutative, $a^2 \in Z$ for every $a \in A^-$. Now, if $a \in A^-$, $k \in K$ then $ak - ka \in A^-$ so $a(ak - ka) = (ak - ka)a$. However, since $a^2 \in Z$, $a(ak - ka) = -(ak - ka)a$. The net result of this is that $2a(ak - ka) = 0$, and so $ak = ka$ for all $a \in A^-$, $k \in K$. But K generates D. Hence we get that $A^- \subset Z$, and so $A \subset Z$.

Thus the theorem is proved if $A^* = A$. Now suppose that A is any subdivision ring such that $uAu^{-1} \subset A$ for every unitary $u \in D$. Let $B = A \cap A^*$; then $B^* = B$ and $uBu^{-1} \subset B$ for every unitary in D.

If A is noncommutative and $\dim_Z D > 16$ and $A \neq D$ or if A is commutative and $\dim_Z D > 4$, by the argument above we know that $B \subset Z$.

If the characteristic of D is not 3, as we pointed out in the paragraph following the proof of Lemma 2, $[A, K] \subset A$ whence, by [2], if A is commutative and $\dim_Z D > 4$ then $A \subset Z$ and if A is not commutative and $\dim_Z D > 16$, then $A = D$. So, to finish the proof, we may assume that D is of characteristic 3.

Our first objective is to show that $aa^* = a^*a$ for $a \in A$. Let $k = a - a^*$; then $ka - ak = aa^* - a^*a$ is symmetric hence $(1 - k)^{-1}(ka - ak)(1 + k)^{-1}$ is symmetric. But, by Lemma 1 it is in A; being symmetric it is also in A^*, hence in $A \cap A^* = B \subset Z$. Thus $\lambda = (1 - k)^{-1}(ka - ak)(1 + k)^{-1} = (1 - k)^{-1}(aa^* - a^*a)(1 + k)^{-1}$, giving us $aa^* - a^*a = \lambda(1 - k^2)$ where $\lambda \in Z$ and $k = a - a^*$. But then $a(a - a^*) - (a - a^*)a = a^*a - aa^*$ commutes with $a - a^*$. Thus, since the characteristic of D is 3, we get $a(a - a^*)^3 = (a - a^*)^3 a$; applying $*$ gives $a^*(a - a^*)^3 = (a - a^*)^3 a^*$. Therefore, if M is the subdivision ring generated over A by a and a^*, then $M^* = M$ and $(a - a^*)^3$ is in the center Z_1 of M. If $a \neq a^*$ we have that the involution is of the *second kind on* M. Also, $A_1 = A \cap M$ is invariant with respect to the unitaries of M. By Lemma 3, if $K_1 = K \cap M$, then $[A_1, K_1] \subset A_1$. Hence since $a \in A_1$ and $a - a^* \in K_1$, $a(a - a^*) - (a - a^*)a \in A$, that is, $aa^* - a^*a \in A$. But $a^*a - aa^*$ is symmetric; hence it is in $A \cap A^* \subset Z$. But we saw earlier that $a^*a - aa^* = \lambda(1 - k^2)$, $\lambda \in Z$, where $k = a - a^*$; thus, if $\lambda \neq 0$ we get $1 - k^2 \in Z$ and so $k^2 \in Z$. Since $k^3 \in Z_1$, we have $k^3 k^{-2} \in Z_1$, so $k \in Z_1$. Thus $a - a^*$ commutes with a, giving us that $aa^* = a^*a$. If $\lambda = 0$ then $aa^* = a^*a$.

We strengthen this last result to, $a^*b = ba^*$ for all $a, b \in A$. For, since $aa^* = a^*a$, $u = a^*a^{-1}$ is unitary. Thus $a^*a^{-1}Aaa^{*-1} \subset A$, and so $a^*Aa^{*-1} \subset A$. Similarly, $(1 + a^*)A(1 + a^*)^{-1} \subset A$. Using Brauer's argument in [1] we have either $a^* \in A$, in which case $a \in Z$, $a^*b = ba^*$, or a^* centralizes A, in which case $a^*b = ba^*$. Thus $a^*b = ba^*$ for all $a, b \in A$.

In particular, if A is commutative then the subdivision ring generated by A and A^* now must be commutative and invariant relative to *. Since it is invariant *re* unitaries, if $\dim_Z D > 4$ we have that it must be in Z; hence $A \subset Z$.

So, to finish, we may assume that A is not commutative, $A \neq D$ and $\dim_Z D > 16$. If $R = \{x \in D \mid xa = ax \text{ all } a \in A\}$ then $uRu^{-1} \subset R$ for all unitaries, R is not commutative since it contains A^*, $R \neq D$ since $A \not\subset Z$. Moreover, $R \supset Z$. We want to show this is impossible. What we have achieved, in going to R, is the fact that $R \supset Z$. Rephrasing, without loss of generality, $A \supset Z$.

The center, Z_0, of A is commutative and invariant with respect to the unitaries, since A is. By what we established earlier, Z_0 must be in Z. Since $Z_0 \supset Z$ we have that the center of A is Z. Thus Z is also the center of A^*.

Our aim, now, is to show that A is 4-dimensional over Z. If $a, c \in A$ and $ac - ca \neq 0$, using $k = c - c^*$ gives $ak - ka = ac - ca \neq 0$. If $b = (ak - ka)^{-1} = (ac - ca)^{-1}$, by Lemma 2, $b - kbk \in A$. Since $b \in A$, we get $(c - c^*)b(c - c^*) \in A$. Expanding this, making use of $cbc \in A$ and c^* centralizes A, we get

$$t = c^*(cb + bc) - c^{*2}b \in A.$$

Therefore $tb - bt \in A$; this results in $c^*(cb^2 - b^2c) \in A$. But $cb^2 - b^2c \neq 0$, (since it is in A) leads to $c^* \in A$, hence $c^* \in A \cap A^* = Z$, and so $c \in Z$. This contradicts $ac - ca \neq 0$. Thus $cb^2 - b^2c = 0$; hence $(ac - ca)^2c = c(ac - ca)^2$ if $ac \neq ca$. This relation is certainly true if $ac = ca$. Therefore A satisfies the polynomial identity $(xy - yx)^2x - x(xy - yx)^2$ of degree 5. By a result of Kaplansky [4], A is at most 4-dimensional over its center Z. Since A is not commutative, A must be 4-dimensional over Z. Thus A^* is also 4-dimensional over Z. Thus $T = AA^*$ is a subring of D (since A^* centralizes A) and is at most 16-dimensional over Z. Consequently T must be a subdivision ring of D. Moreover, $T^* = T$, $uTu^{-1} \subset T$ for all unitaries and T is not commutative since $T \supset A$. But then we have seen, since $\dim_Z D > 16$, that T must equal D. This would lead to the contradiction $16 < \dim_Z D = \dim_Z T \leqslant 16$. With this, the theorem is proved.

References

1. Richard Brauer, On a theorem of H. Cartan, *Bull. Amer. Math. Soc.* **55** (1949), 619–620.

2. I. N. HERSTEIN, Invariant submodules of simple rings with involution, (to appear).
3. I. N. HERSTEIN, "Topics in Ring Theory," University of Chicago Press, Chicago, Ill., 1969.
4. IRVING KAPLANSKY, Rings with polynomial identity, *Bull. Amer. Math. Soc.* **54** (1948), 575–580.